AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Subject devices in the custody of Kirkland Police Department, further described in Attachment A	)	Case No. MJ18-220

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Subject devices as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, U.S.C. §§ 371, 1349	Conspiracy
Title 18, U.S.C. § 1029	Access Device Fraud
Title 18, U.S.C. § 1343	Wire Fraud

The application is based on these facts:

See attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of ____ days (give exact ending date if more than 30 days: ____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SPECIAL AGENT COLBY GARCIA, USSS

Printed name and title

Sworn to before me pursuant to CrimRule 4.1.

Date: 05/11/2018

Judge's signature

City and state: SEATTLE, WASHINGTON

BRIAN A. TSUCHIDA, CHIEF U.S. MAGISTRATE JUDGE

Printed name and title

2017R01248

ATTACHMENT A

SUBJECT DEVICES TO BE SEARCHED

a. HP Laptop, Serial #: 5CB4239QD;

b. Lenovo B570-1068 Laptop, Serial #WB03647224;

c. Canon PIXMA-MG3620 Printer, Serial #KLDH98125;

d. Seagate 2TB Hard Drive, Serial #WDZ7Y6MD;

e. WD 750GB Hard Drive, Serial #WXD1EB3JXPG7;

f. WD 500GB Hard Drive, Serial #WXM1A81U4171;

g. Scandisk 16GB USB Flash Drive, Serial#BL170525258B;

h. Samsung Galaxy Note 5 Cell Phone, IMEI: 353876070954017;

i. Apple Iphone Cell Phone, IMEI: 356600080235549;

j. Samsung Galaxy Note Cell Phone, Serial#RV1D956TFNR;

k. Go-Pro Hero 5 Camera;

l. Samsung Cell Phone, MEDI HEX #A000003991271D; and

m. Samsung Cell Phone, MEDI HEX #A0000039E641EC.

All of the aforementioned items or devices are currently in the custody of the Kirkland Police Department, located in Kirkland, Washington

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 981012
(206) 553-7970

ATTACHMENT B

ITEMS TO BE SEIZED

All evidence on the SUBJECT DEVICES described in Attachment A that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. §§ 371 and 1349 (Conspiracy), 18 U.S.C. § 1029 (Access Device Fraud), 18 U.S.C. § 1343 (Wire Fraud) (collectively, the "Subject Offenses"), for the time period of **January 1, 2017 to December 1, 2017**, including:

a. Documents, records or files relating to the identification of the individuals committing the Subject Offenses

b. Documents, records or files relating to credit/debit card, gift card, or account or card numbers;

c. Documents, records or files relating to planned, attempted, or successful use of gift cards or card data to conduct purchases or transactions;

d. Documents, records or files relating to the purchase, receipt, manufacture, maintenance, or use of card-reading or encoding equipment or software, device-making equipment;

e. Documents, records or files relating to the creation, manufacture, possession, transfer, or use of counterfeit cards or stolen card data, including the Luhn algorithm software or files that may be used for encoding and/or re-encoding gift cards;

f. Documents, records or files relating to or referencing Target, transactions conducted at Target, items or services purchased from Target, or communications about Target or with Target representatives;

g. Documents, records or files relating to online vendors, such as Paxful, where gift cards and gift card balances may be listed, sold, or purchased;

h. Documents, records or files relating to cryptocurrency, such as Bitcoin, and the use and possession thereof, including any wallets and passcodes and public/private keys thereto;

i. Documents, records or files indicating dominion and control;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 981012
(206) 553-7970

j. Documents, records or files relating to the deposit, withdrawal, or transfer of funds, including, but not limited to, wire transfers;

k. Photographs depicting cash, cards/card stock, device-making equipment, transactions, and/or any other individual that may be involved in the criminal scheme;

l. Documents, records or files establishing criminal associations, including address books, contact lists, and telephone or communication records;

m. Documents, records or files relating to software, programs or applications, such as Pocket Zee, that enables the use of gift cards or gift card numbers on digital devices;

n. Documents, records or files relating to the use or sale of items purchased using stolen Target gift card numbers;

o. Evidence of user attribution showing who used or owned the SUBJECT DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, contact lists, saved usernames and passwords, documents, pictures/photographs, and browsing history;

p. Records and/or data that may reveal the past location of the individual or individuals using the SUBJECT DEVICES;

q. Any passwords, password files, test keys, encryption codes or other information necessary to access computer equipment, storage devices or data.

r. For each of the SUBJECT DEVICES:

i. Evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

ii. Evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 981012
(206) 553-7970

of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. Evidence of the lack of such malicious software;

iv. Evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

v. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

vi. Evidence of the times the digital device or other electronic storage media was used;

vii. Passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;

viii. Documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;

ix. Contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "documents, "records," and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 981012
(206) 553-7970

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, Colby Garcia, being first duly sworn on oath, depose and say:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent (SA) with the United States Secret Service (USSS) and have been so since August 24, 2016. I am currently assigned to the Seattle Field Office. Previously, I was a commissioned Law Enforcement Officer for 5 years, serving as a patrol officer with the Atlanta Police Department and the Alpharetta Police Department in Fulton County, Georgia.

2. I am a graduate of the Federal Law Enforcement Training Center (FLETC) located in Glynco, Georgia, and the Secret Service Special Agent Training Program located in Beltsville, Maryland. As part of my training with the Secret Service, I have received instruction on the investigation of financial crimes, including credit/debit card fraud, mail and wire fraud, access device fraud, and identity theft. In the course of my law enforcement career, I have investigated crimes ranging from the production and passing of counterfeit currency, identity theft, access device fraud, bank fraud and threats made against the President and Vice President of the United States. I have a Bachelor of Arts degree from the University of Georgia.

3. I am familiar with, and have participated in, a variety of investigative techniques including, but not limited to, analysis of documentary and financial evidence, surveillance, the questioning of witnesses, the implementation of undercover operations, and execution of search and seizure warrants.

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 981012
(206) 553-7970

4. I make this Affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the following digital devices[1] and other electronic storage media[2] (hereinafter "SUBJECT DEVICES"), as more fully described in ATTACHMENT A to this Affidavit, for the items described in ATTACHMENT B to this Affidavit, which are incorporated herein by reference:

a) HP Laptop, Serial #5CB4239QD;
b) Lenovo B570-1068 Laptop, Serial #WB03647224;
c) Canon PIXMA-MG3620 Printer, Serial #KLDH98125;
d) Seagate 2TB Hard Drive, Serial #WDZ7Y6MD;
e) WD 750GB Hard Drive, Serial #WXD1EB3JXPG7;
f) WD 500GB Hard Drive, Serial #WXM1A81U4171;
g) Scandisk 16GB USB Flash Drive, Serial #BL170525258B;
h) Samsung Galaxy Note 5 Cell Phone, IMEI: 353876070954017;
i) Apple IPhone Cell Phone, IMEI: 356600080235549;
j) Samsung Galaxy Note Cell Phone, Serial#RV1D956TFNR;
k) Go-Pro Hero 5 Camera;
l) Samsung Cell Phone, MEDI HEX #A00000391271D; and
m) Samsung Cell Phone, MEDI HEX #A0000039E641EC.

5. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; review of documents and records

[1] "Digital device" includes any electronic device capable of processing and/or storing data in digital form, including, but not limited to: central processing units, laptop or notebook computers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, cables and connections, and electronic/digital security devices wireless communication devices such as telephone paging devices, beepers, mobile or cellular telephones, personal data assistants ("PDAs"), iPods, blackberries, digital cameras, digital gaming devices.

[2] Electronic Storage media is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 981012
(206) 553-7970

related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience.

6. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation. I have set forth only facts that I believe are sufficient to the determination of probable cause to believe that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 and 1349 (Conspiracy), 18 U.S.C. § 1029 (Access Device Fraud), and 18 U.S.C. § 1343 (Wire Fraud) (collectively, the "Target Offenses"), will be found on the SUBJECT DEVICES.

7. The requested warrant would authorize the forensic examination of the SUBJECT DEVICES for the purpose of identifying electronically stored information (ESI) particularly described in Attachment B.

8. The SUBJECT DEVICES are currently in the lawful possession of the Kirkland Police Department (KPD), located in Kirkland, Washington, and were seized through the investigation, as described herein.

9. The SUBJECT DEVICES are currently in storage at the KPD evidence facility. In my training and experience, and based upon my involvement in this investigation, I know that the SUBJECT DEVICES have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the SUBJECT DEVICES first came into the possession of KPD, as discussed below.

This Affidavit is being presented electronically pursuant to Local Criminal Rule CrR 41(d)(3).

SUMMARY OF INVESTIGATION

10. As discussed in more detail below, this investigation relates to an elaborate fraudulent scheme that compromised the gift card system of a particular U.S. retailer,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 981012
(206) 553-7970

causing multiple hundreds of thousands of dollars (to date, at least approximately $760,000) in loss. In short, a group of individuals, including Jeffery Mann and numerous others, some of whom are identified herein, reverse-engineered gift card numbers, which they used to make unauthorized purchases at various Target retail stores in the Western District of Washington and elsewhere.

11. Target Corporation ("Target") began an investigation on or about June 8, 2016, when Market Investigator Derek Forare became aware of fraudulent gift card activity impacting guests in Target stores in Western Washington. According to Forare, he was notified by Target's Lynnwood, Washington store team leader, Brandon Bogart, about possible fraud activity at the Lynnwood store. Bogart reported seeing suspicious transactions conducted by subjects over the preceding few days. These transactions involved multiple gift card numbers scanned from cell phones[3] to conduct high-dollar transactions.

12. Bogart had identified one of the subjects as "Jeremy" Mann who was involved with an incident at the store on April 20-21, 2017, involving a suspicious vehicle in the parking lot. He was later identified as Jeffery Mann through comparison of surveillance footage with his social media profile and communication with Lynnwood Police Department, which was aware of Jeffery Mann.

13. After receiving this information, Forare contacted Target's National Investigation Center and learned that Target had received several complaints in early June 2017 from customers who were missing balances from their Target gift cards, and Target was already working at corporate headquarters to investigate and gather information on the subjects involved in the fraud.

14. On June 10, 2017, Bogart (the Lynnwood store team leader) observed a group of four subjects attempt to make a $900.00 purchase using gift cards on their cell phones at Target. Bogart was able to speak with the subjects in person at the cash

[3] As described herein, in addition to traditional cards, gift card balances can be accessed and used through various electronic means, such as applications available on digital devices.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 981012
(206) 553-7970

register and provide guest service. Bogart immediately recognized one subject as Jeffery Mann from the previous incident at Target on April 21, 2017, and from the June 8, 2017, incident described above. The other male that was with Mann was identified as Corey Mosey, who had also been involved, and identified, in the April 21, 2017 suspicious vehicle incident. In addition to Mann and Mosey, two females also accompanied them at the cash register. One female was later identified by Forare as Danielle Helm by matching her appearance on Target surveillance footage with images captured from her social media profiles. While Bogart talked with the subjects, he observed a mobile phone application open on the screen of one of their cell phones called "Pocket Zee." According to Forare, Pocket Zee is a third-party mobile wallet application for a cell phone. It is unaffiliated with Target. The application allows a user to input a gift card number into the program, and creates a barcode image that can be scanned at Target registers at the time of purchase. Bogart denied the sale and the subjects exited the store.

15. On June 13, 2017, Forare was advised by the Bellingham, Washington store assets protection leader that individuals were observed at a Target store in Bellingham, Washington making purchases with multiple gift cards. Forare was able to match surveillance footage from Bellingham to the individual identified as Mann. According to Forare, Mann used several Target gift cards scanned from his cell phone to purchase an iTunes gift card.

16. According to Target investigators, including Forare and Target Special Investigator Alex Glistsos, the subjects involved in the fraud activity were not tampering with physical cards or taking photos of the barcodes in Target stores, as the compromised gift card balances included gift cards sold online at Target.com and those purchased by guests in other states throughout the country. Instead, the subjects had been able to decode the gift card numbers using something known as a Luhn algorithm, then create barcodes (using the third-party mobile wallet application) corresponding to the gift card numbers they obtained—numbers on gift cards that are sold or issued to guests every day. By doing this, the perpetrators were able to duplicate gift card barcodes without ever

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 981012
(206) 553-7970

being in possession of the cards themselves. Target investigators also believed the subjects created gift card barcodes by starting with a known, working, gift card barcode and working backwards with the number sequence or algorithm, knowing that the previous gift card numbers had likely already been issued.

17. Based on information gathered on June 13, 2017, including surveillance and transaction records that included the names or emails of suspected perpetrators, Target's National Investigation Center was able to conduct social media searches and determine the identities of a number of subjects involved. The main group of subjects involved in the activity as of that date included: Jeffery Mann (4/7/1989), Corey Mosey (10/11/1987), Samantha Fleischacker (1/25/1992), Kayle McCrary (11/16/1992), Justin Brown (9/17/1993), Danielle Helm (8/19/1991), and Derrick Quintana (3/25/1992). Connections to each other and their involvement in the gift card fraud were developed from observations of their joint presence in various stores where they conducted transactions with gift card numbers scanned from their phones, as well as pictures on social media showing subjects together.

18. On June 16, 2017, Forare contacted Detective Brad Reorda of the Lynnwood Police Department, and discussed the activity of Mann and the other subjects believed to be involved with Mann's fraudulent activity. According to Forare, Detective Reorda stated he was familiar with Mann and the other subjects, and explained that they are a transient group who are known to stay at different hotels.

19. On July 26, 2017, subjects Jeffery Mann, Derrick Quintana, and Lindsay Brandner were contacted by Marysville Police Department in a Motel 6 hotel room in Everett, Washington, during the unrelated arrest of a fourth individual also present in the room. According to police reports, officers identified a rented Jeep associated with the group, which Mann identified as belonging to him. Officers searched the hotel room and Jeep pursuant to warrants, and located gift card ledgers and worksheets, dozens of gift cards, including for Target, Steam.com, Hotels.com, and other retailers, a magnetic reader-writer, and financial paperwork and identifying documents belonging to third

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 981012
(206) 553-7970

parties. Among the ledgers were lists of what Forare was able to recognize as Target gift card numbers, written in sequence, and notes taken on the card balances or descriptions. Among the notebooks, there was a note saying, "don't say anything about me teaching you b/c/ Jeff gets made cause he taught us." There were also notes related to the sale of a vehicle from "Kennady Weston" to another person, and the debt owed to "Kennady" as of March 23, 2017.

20. On August 7, 2017, Forare emailed me that Mann and other subjects were travelling, and transactions at Target stores were made in Las Vegas, Nevada and Portland, Oregon in the last few days. Surveillance video from Target stores in the Las Vegas area in early August 2017 show transactions conducted by shoppers matching the physical attributes of subjects Jeffery Mann and Kennady Weston, using scans of cellular telephones to make purchases. Facebook posts from Derrick Quintana in August 2017 show photos and videos of Quintana with individuals identified through social media profiles as Mann and Kennady Weston in what appears from the photos and videos to be Las Vegas. Records from Expedia show that, later in August 2017, the email address associated with Samantha Fleishacker's Facebook profile was used to book rooms in Las Vegas, with the registered guest identified as Derrick Quintana.

21. I learned that on August 5, 2017, three subjects—Corey Mosey, Kayle McCrary, and Timothy Brand—were arrested in Oregon by officers with the West Linn Police Department. According to police reports, Brand was arrested initially for DUI, and officers discovered gift cards and other newly purchased merchandise with him (and passenger Mosey) in the car. Brand told officers that Mosey used the Luhn algorithm and the last few digits of a gift card number to see if the card was active or not. Brand admitted he (Brand) would go into Target stores and buy things with the fraudulent gift cards. Brand also identified Jeff Mann as the ringleader of the gift card operation and said that Mann was headed to Las Vegas (as noted above, Target Surveillance and social media posts show Mann in Las Vegas in early August 2017). Officers obtained consent from Kayle McCrary and Corey Mosey to search the Motel 6 where they, and Brand,

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 981012
(206) 553-7970

were staying. During the search they found Target gift cards with remaining balances written on the back, notebooks with apparent gift card numbers from various retailers. McCrary admitted to keeping records of the gift card numbers that were used, calling Target to determine balances, and transferring balances to applications on her cell phone.

22. Through its investigation, Target has identified and preserved surveillance footage of hundreds of transactions by individuals matching the physical characteristics of the subjects named in this Affidavit, including Jeffery Mann, Corey Mosey, Samantha Fleishacker, Derrick Quintana, Hayley Brown, Justin Brown, Danielle Helm, and numerous others. Based on Target records, these transactions typically involve the use of multiple gift card numbers to complete the purchase. As part of my investigation, I have reviewed such surveillance footage and records obtained from Target. In many instances, the footage shows the individual using that barcode scanner at the Target register on his or her cell phone. In some instances, the individual uses traditional (counterfeit) physical cards to conduct the transaction. Based on my training and experience, and that of other experienced investigators, I know that creating counterfeit cards often involves use of various digital devices, including computers, printers, and other devices.

23. On November 30, 2017, I learned that Kirkland Police Department (KPD) had Jeffery Mann in custody following an arrest for fraud, and I notified KPD Detective Frankeberger that Mann was the main subject in a Secret Service investigation. At approximately 7:00pm, I met Detective Sean Carlson and Detective Frankeberger at KPD. Target investigator Derek Forare was also present at KPD, and described to detectives Target's involvement in the case. Forare advised the KPD detectives that he and a corporate intelligence group had compiled an extensive investigation that had identified Mann as the leader of a group conducting gift card fraud in Washington, Nevada, Colorado, California, and Oregon. Forare also disclosed that the estimated total loss to Target (reimbursements to defrauded customers) as a result of the compromised gift cards totaled approximately $760,000, roughly $517,000 of which occurred in Washington State, since May of 2017.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 981012
(206) 553-7970

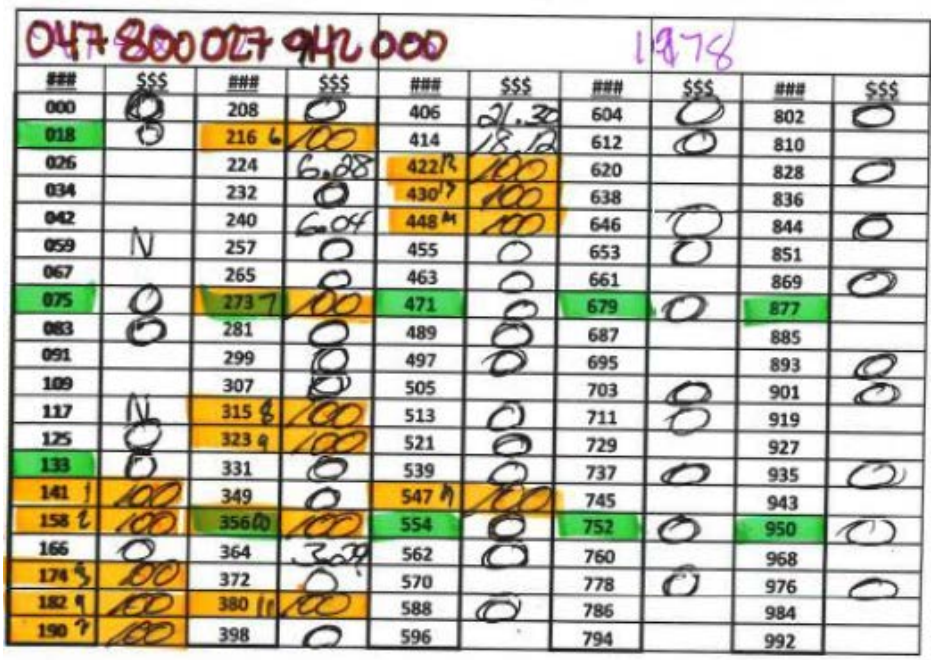
24. Along with Detective Frankeberger, I interviewed Mann. After waiving his *Miranda* rights, Mann explained that he and his friend "Corey" had figured out that the barcodes for Target gift cards were determined by an algorithm. Using that algorithm (the "Luhn algorithm") enabled him to deduce what the gift card numbers for a given set or sequence of Target gift cards were likely to be. Mann said that Target was easy (or easier than some other retailers' gift cards) because it was only a barcode, and Target did not require an Access Number or PIN, and did not use random numbers. He explained that he and others participating in the scheme would get a gift card, scan it to get the numbers, and then work out the gift card numbers for other cards. He would call to check those numbers for fund balances, and then would add those numbers with a usable balance to his phone and make a barcode he could scan. Mann said he would then go to a Target store and purchase gift cards for Steam, Target, and other retailers. He would then re-sell these illegally purchased gift cards through online vendors, such as www.paxful.com, in exchange for cryptocurrency, to include Bitcoin. Mann admitted to operating this scheme for the past six months (from roughly June 1, 2017) in several different states. He admitted doing it at multiple different Target stores in the metropolitan areas of each of Las Vegas, Denver, and Los Angeles, as well as an unknown number of stores in the greater Seattle area. Asked who else was involved, he said maybe 20 people he knows, and others that Corey knows. He gave the names of Hayley Brown, Kennady Weston and Derrick Quintana. Mann also estimated that he had personally profited over $50,000.00.

25. At the time of his arrest by KPD, Mann was driving a gold Volvo sedan. After his arrest, and with Mann's consent, officers searched the Volvo and located, among other things:

- Numerous receipts from Target involving dozens of gift card transactions.
- Dozens and dozens of gift cards from Target, Steam and other vendors, some in packaging, some not.
- Laminating film.
- Blank gift card stock.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 981012
(206) 553-7970

- At least a dozen grids similar to the one pictured below. The grids had different numbers across the topline and were in various states of completion.



###	$$$	###	$$$	###	$$$	###	$$$	###	$$$
000		208		406		604		802	
018		216		414		612		810	
026		224		422		620		828	
034		232		430		638		836	
042		240		448		646		844	
059		257		455		653		851	
067		265		463		661		869	
075		273		471		679		877	
083		281		489		687		885	
091		299		497		695		893	
109		307		505		703		901	
117		315		513		711		919	
125		323		521		729		927	
133		331		539		737		935	
141		349		547		745		943	
158		356		554		752		950	
166		364		562		760		968	
174		372		570		778		976	
182		380		588		786		984	
190		398		596		794		992	

26. KPD Officers learned from Totem Lake Hotel that Mann was the registered guest of room 155, and had been renting that room for several weeks. Officers applied for and were granted a search warrant for the room. During that search, they located, among other things:

- Hundreds of gift cards, mostly from Target and Steam, both opened and unopened.
- Dozens of receipts from Target and Target shopping bags.
- Dozens of grids used to track and organize large blocks of gift card numbers in a series.
- A black HP laptop, powered on. The screen displayed applications named “templates”, “barcode generator”, “password decryption”, “DYMO Label”, etc.
- Numerous journals and notebooks containing series of number appearing to be account or gift card numbers. One included a phone number (1-800-544-2943), which officers confirmed is for Target Gift Card Services.
- A label maker.
- Court documents for Mann.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 981012
(206) 553-7970

- A vehicle title application for Mann's Volvo.
- A large bag of shredded aluminum that appears that it may be shredded credit or gift cards.
- Sheets of barcodes and photocopied gift cards.

27. All of the SUBJECT DEVICES described in this Affidavit were located in either Jeffery Mann's Volvo, or in his hotel room. The SUBJECT DEVICES were transported to KPD and processed and booked into evidence storage, where they have remained to date.

28. Jeffery Mann was arrested and later charged in King County Superior Court.

DEFINITIONS AND TECHNICAL TERMS

29. Set forth below are some definitions of technical terms, most of which are used throughout this Affidavit pertaining to the Internet and computers generally. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Computers and digital devices: As used in this Affidavit, the terms "computer" and "digital device," along with the terms "electronic storage media," "digital storage media," and "data storage device," refer to those items capable of storing, creating, transmitting, displaying, or encoding electronic or digital data, including computers, hard drives, thumb drives, flash drives, memory cards, media cards, smart cards, PC cards, digital cameras and digital camera memory cards, electronic notebooks and tablets, smart phones and personal digital assistants, printers, scanners, and other similar items.

b. Wireless/cellular telephone: A wireless or cellular telephone (or mobile telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 981012
(206) 553-7970

In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

c. Electronic Storage media: Electronic Storage media is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The GPS consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

FORENSIC ANALYSIS

30. Based on my training, experience, and research, and from consulting with others, I know that the SUBJECT DEVICES have capabilities that allow them to serve as electronic storage devices of information and data and, in some cases, instrumentalities of criminal conduct. For example, a GPS navigation device on the various cell phones

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 981012
(206) 553-7970

could hold historical information about the device's whereabouts and location searches, which may serve as evidence and/or assist law enforcement in identifying other co-conspirators, among other things. The various cell phones may also include records of communications between and among co-conspirators, including text messages or voicemails directly regarding the commission of the Target Offenses. And, of course, the laptop computer, hard drives, and memory cards may hold data relating to gift card numbers. Finally, in my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

31. Based on my knowledge, training and experience, I know that digital devices and electronic storage media can store information for long periods of time. Similarly, things that have been viewed via the Internet are typical stored for some period of time on the device used to access the Internet. This information can sometimes be recovered with forensic tools.

32. There is probable cause to believe that things that were once stored on the SUBJECT DEVICES may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a digital device or other electronic storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a digital device or other electronic storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the digital device or other electronic storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the digital device or other electronic storage medium that is not currently being used by an active file—for long periods of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 981012
(206) 553-7970

time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

33. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only ESI that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the SUBJECT DEVICES were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the SUBJECT DEVICES because:

a. Data on a digital device or other electronic storage medium can provide evidence of a file that was once on the digital device or other electronic storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the digital device or other electronic storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 981012
(206) 553-7970

was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner and/or others with direct physical access to the computer. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.[4] Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of

[4] For example, if the examination of a computer shows that: a) at 11:00am, someone using the computer used an internet browser to log into a bank account in the name of John Doe; b) at 11:02am the internet browser was used to download child pornography; and c) at 11:05 am the internet browser was used to log into a social media account in the name of John Doe, an investigator may reasonably draw an inference that John Doe downloaded child pornography.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 981012
(206) 553-7970

other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., Internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a digital device or other electronic storage medium works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how the devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a digital device or other electronic storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 981012
(206) 553-7970

34. Manner of execution. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

DIGITAL DEVICES AS INSTRUMENTALITIES OF THE CRIMES

35. I know that when an individual uses a digital device or other electronic storage medium to download, store, transfer, or download or upload card data or other victim-related information, the individual's device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a digital device or other electronic storage medium used to commit a crime of this type may contain: data that is evidence of how the device was used; data that was sent or received; and other records that indicate the nature of the offense.

PRIOR EFFORTS TO OBTAIN EVIDENCE

36. Alternative methods of obtaining the evidence sought after have been reasonably exhausted. At this time, any other means of obtaining the necessary evidence could result in an unacceptable risk of the loss/destruction of the evidence sought. Based on my knowledge, training and experience, the only effective means of collecting and preserving the required evidence in this case is through a search warrant.

SEARCH TECHNIQUES

37. Based on the foregoing, and consistent with Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, the warrant I am applying for will permit imaging or otherwise copying all data contained on the SUBJECT DEVICES, and will specifically authorize a review of the media or information consistent with the warrant. The review may require techniques, including computer-assisted scans of the media or information

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 981012
(206) 553-7970

that might expose many parts of the media or information to human inspection in order to determine whether it contains the items described in Attachment B.

38. In accordance with the information in this affidavit, law enforcement personnel will execute the search of the SUBJECT DEVICES pursuant to this warrant as follows:

a. Securing the Data

i. In order to examine the ESI in a forensically sound manner, law enforcement personnel with appropriate expertise will attempt to produce a complete forensic image, if possible and appropriate, of the SUBJECT DEVICES.[5]

ii. A forensic image may be created of either a physical drive or a logical drive. A physical drive is the actual physical hard drive that may be found in a typical computer. When law enforcement creates a forensic image of a physical drive, the image will contain every bit and byte on the physical drive. A logical drive, also known as a partition, is a dedicated area on a physical drive that may have a drive letter assigned (for example the c: and d: drives on a computer that actually contains only one physical hard drive). Therefore, creating an image of a logical drive does not include every bit and byte on the physical drive. Law enforcement will only create an image of physical or logical drives physically present on or within the SUBJECT DEVICES. Creating an image of the SUBJECT DEVICES will not result in access to any data physically located elsewhere. However, SUBJECT DEVICES that have previously connected to devices at other locations may contain data from those other locations.

[5] The purpose of using computer personnel to conduct the imaging of digital devices is to ensure the integrity of the evidence and to follow proper, forensically sound, scientific procedures. When the investigative agent is a trained computer examiner, it is not always necessary to separate these duties. Prior to recent court-imposed limitations on the conduct of ESI search warrants, computer personnel typically worked closely with investigative personnel in all investigations involving digital evidence to assist investigators in their search for digital evidence. The point of using computer personnel to segregate data in a digital investigation was typically technological rather than legal. Computer personnel are needed because they generally have technological expertise that investigative agents do not possess. Computer personnel, however, typically lack the factual and investigative expertise that an investigative agent may possess on any given case. Therefore, it is important that computer personnel and investigative personnel work closely together. In more complex computer investigations, especially those involving computer intrusions, law enforcement will often assign an investigative agent with training and experience in computer examinations and/or computer science because of the importance of combining the investigative and technological skills.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 981012
(206) 553-7970

b. Searching the Forensic Images

i. Searching the forensic images for the items described in Attachment B may require a range of data analysis techniques. In some cases, it is possible for agents and analysts to conduct carefully targeted searches that can locate evidence without requiring a time-consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant, and law enforcement may need to conduct more extensive searches to locate evidence that falls within the scope of the warrant. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this affidavit.

ii. The search techniques that will be used will be only those methodologies, techniques and protocols as may reasonably be expected to find, identify, segregate and/or duplicate the items authorized to be seized pursuant to Attachment B to this affidavit. These methodologies, techniques and protocols may or may not include the use of a "hash value" library to exclude normal operating system files that do not need to be further searched. Or, agents may utilize hash values to exclude certain known files, such as the operating system and other routine software, from the search results. However, because the evidence I am seeking does not have particular known hash values, agents will not be able to use any type of hash value library to locate the items identified in Attachment B.

39. Manner of execution. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 981012
(206) 553-7970

REQUEST FOR SEALING

40. It is respectfully requested that this Court issue an order sealing all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation into criminal organizations and not all of the targets of this investigation, including several persons identified herein, will be searched at this time. Based upon my training and experience, I have learned that, some criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other others as they deem appropriate, i.e., post them publicly online through the carding forums. This is of particular importance here, where the criminal conspiracy at issue involves numerous persons, many who remain unidentified, and conduct outside the United States. Moreover, the investigation has utilized and continues to utilize cooperating co-conspirators. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

//

//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 981012
(206) 553-7970

CONCLUSION

41. Based on the foregoing, I believe there is probable cause that evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 371 and 1349 (Conspiracy), 18 U.S.C. § 1029 (Access Device Fraud), and 18 U.S.C. § 1343 (Wire Fraud), are located in the SUBJECT DEVICES, as more fully described in Attachment A to this Affidavit. I therefore request that the court issue a warrant authorizing a search of the SUBJECT DEVICES for the items more fully described in Attachment B hereto, incorporated herein by reference, and the seizure of any such items found therein.

COLBY GARCIA, Affiant
Special Agent
United States Secret Service

The above-named agent provided a sworn statement attesting to the truth of the contents of the foregoing affidavit on 11th day of May, 2018.

BRIAN A. TSUCHIDA
Chief United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 981012
(206) 553-7970

ATTACHMENT A

SUBJECT DEVICES TO BE SEARCHED

a. HP Laptop, Serial #: 5CB4239QD;

b. Lenovo B570-1068 Laptop, Serial #WB03647224;

c. Canon PIXMA-MG3620 Printer, Serial #KLDH98125;

d. Seagate 2TB Hard Drive, Serial #WDZ7Y6MD;

e. WD 750GB Hard Drive, Serial #WXD1EB3JXPG7;

f. WD 500GB Hard Drive, Serial #WXM1A81U4171;

g. Scandisk 16GB USB Flash Drive, Serial#BL170525258B;

h. Samsung Galaxy Note 5 Cell Phone, IMEI: 353876070954017;

i. Apple Iphone Cell Phone, IMEI: 356600080235549;

j. Samsung Galaxy Note Cell Phone, Serial#RV1D956TFNR;

k. Go-Pro Hero 5 Camera;

l. Samsung Cell Phone, MEDI HEX #A000003991271D; and

m. Samsung Cell Phone, MEDI HEX #A0000039E641EC.

All of the aforementioned items or devices are currently in the custody of the Kirkland Police Department, located in Kirkland, Washington

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 981012
(206) 553-7970

ATTACHMENT B

ITEMS TO BE SEIZED

All evidence on the SUBJECT DEVICES described in Attachment A that constitutes fruits, contraband, evidence and instrumentalities of violations of 18 U.S.C. §§ 371 and 1349 (Conspiracy), 18 U.S.C. § 1029 (Access Device Fraud), 18 U.S.C. § 1343 (Wire Fraud) (collectively, the "Subject Offenses"), for the time period of **January 1, 2017 to December 1, 2017**, including:

a. Documents, records or files relating to the identification of the individuals committing the Subject Offenses

b. Documents, records or files relating to credit/debit card, gift card, or account or card numbers;

c. Documents, records or files relating to planned, attempted, or successful use of gift cards or card data to conduct purchases or transactions;

d. Documents, records or files relating to the purchase, receipt, manufacture, maintenance, or use of card-reading or encoding equipment or software, device-making equipment;

e. Documents, records or files relating to the creation, manufacture, possession, transfer, or use of counterfeit cards or stolen card data, including the Luhn algorithm software or files that may be used for encoding and/or re-encoding gift cards;

f. Documents, records or files relating to or referencing Target, transactions conducted at Target, items or services purchased from Target, or communications about Target or with Target representatives;

g. Documents, records or files relating to online vendors, such as Paxful, where gift cards and gift card balances may be listed, sold, or purchased;

h. Documents, records or files relating to cryptocurrency, such as Bitcoin, and the use and possession thereof, including any wallets and passcodes and public/private keys thereto;

i. Documents, records or files indicating dominion and control;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 981012
(206) 553-7970

j. Documents, records or files relating to the deposit, withdrawal, or transfer of funds, including, but not limited to, wire transfers;

k. Photographs depicting cash, cards/card stock, device-making equipment, transactions, and/or any other individual that may be involved in the criminal scheme;

l. Documents, records or files establishing criminal associations, including address books, contact lists, and telephone or communication records;

m. Documents, records or files relating to software, programs or applications, such as Pocket Zee, that enables the use of gift cards or gift card numbers on digital devices;

n. Documents, records or files relating to the use or sale of items purchased using stolen Target gift card numbers;

o. Evidence of user attribution showing who used or owned the SUBJECT DEVICES at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, contact lists, saved usernames and passwords, documents, pictures/photographs, and browsing history;

p. Records and/or data that may reveal the past location of the individual or individuals using the SUBJECT DEVICES;

q. Any passwords, password files, test keys, encryption codes or other information necessary to access computer equipment, storage devices or data.

r. For each of the SUBJECT DEVICES:

i. Evidence of who used, owned, or controlled the digital device or other electronic storage media at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

ii. Evidence of software that would allow others to control the digital device or other electronic storage media, such as viruses, Trojan horses, and other forms

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 981012
(206) 553-7970

of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

iii. Evidence of the lack of such malicious software;

iv. Evidence of the attachment to the digital device of other storage devices or similar containers for electronic evidence;

v. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the digital device or other electronic storage media;

vi. Evidence of the times the digital device or other electronic storage media was used;

vii. Passwords, encryption keys, and other access devices that may be necessary to access the digital device or other electronic storage media;

viii. Documentation and manuals that may be necessary to access the digital device or other electronic storage media or to conduct a forensic examination of the digital device or other electronic storage media;

ix. Contextual information necessary to understand the evidence described in this attachment.

As used above, the terms "documents, "records," and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 981012
(206) 553-7970